UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Susan M. Reichert, on behalf of herself individually and on behalf of all others similarly situated, Plaintiff, v. Netgain Technology, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

The allegations made in this Class Action Complaint are based upon information and belief except those allegations that pertain to Plaintiff, which are based on personal knowledge. Each allegation either has evidentiary support or, alternatively, pursuant to Rule 11(b)(3) of the Federal Rules of Civil Procedure, is likely to have evidentiary support after a reasonable opportunity for further investigation or discovery.

INTRODUCTION

1. Plaintiff Susan Reichert ("Plaintiff") brings this proposed class action on behalf of herself individually and on behalf of all others similarly situated, by and through her attorneys, against Defendant Netgain Technology, LLC ("Netgain" or "Defendant") for its failure to secure and safeguard the confidential, personally identifiable information of hundreds of thousands of consumers. Although the information stolen may vary by individual class member, the categories included names, account numbers, Social Security numbers, driver's license numbers, bank account numbers, and dates of birth ("PII"), as well as personal health information such as medical record numbers, health insurance policy and identification

numbers, clinical notes, referral requests, laboratory results, immunization information, medical disclosure logs, in addition to other medical and health related information ("PHI").

2. Netgain provides cloud-enabled IT solutions and managed services to various types of business entities including healthcare providers and accounting companies.

3. Netgain has provided IT solutions for organizations for nearly 20 years, with offices and data centers located in Chicago, Minneapolis, San Diego, and Phoenix. With approximately 130 employees across its locations, Netgain generates $32.35 million dollars in sales.[1]

4. Indeed, Netgain offers cybersecurity solutions, yet failed to secure its own systems from cybercriminals.

5. In late September 2020, and due to Netgain's inadequate data security and failure to comply with federal and state data privacy standards, an unauthorized third party used compromised credentials to gain access to Netgain's digital environment. Thereafter, the unauthorized third-party gained access to, and then exfiltrated, the files and records of various businesses that are customers of Netgain, including Neighborhood Healthcare, Health CenterPartners of Southern California, Woodcreek Provider Services, LLC, Apple Valley Clinic/Allina Health, Ramsey County, Sandhills Medical Foundation, and Crystal Practice Management.

[1] https://www.dnb.com/business-directory/company-profiles.netgain_technology_llc.52f33163cb3c315c73f15169f269e977.html (last accessed May 26, 2021).

6. In late September 2020, an unidentified third-party launched a ransomware attack against Netgain using the data exfiltrated. Netgain was then forced to take some of its data centers offline as a protective measure in an effort to contain the threat and restore services. Netgain reportedly paid a ransom of $2.3 million to the cybercriminals to restore its systems and for assurances that they would delete all copies of the data obtained and further would not publish, sell, or otherwise disclose the data. This series of events is referred to in this Complaint as the "Data Breach."

7. Due to Netgain's negligence and inadequate data security, Plaintiff and Class members have suffered irreparable harm and are subject to an increased risk of identity theft. Plaintiff and Class members' PII and PHI have been compromised and they must now undertake additional security measures to minimize the risk of identity theft.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

9. This Court has jurisdiction over Defendant because Netgain Technology, LLC maintains its principal place of business in Minnesota, regularly conducts business in Minnesota, and has sufficient minimum contacts in Minnesota. Defendant intentionally availed itself of this jurisdiction by marketing and selling products and services from Minnesota to many businesses nationwide.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant Netgain Technology, LLC's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

PARTIES

11. Plaintiff Susan Marie Reichert is a resident of Cable, Wisconsin and brings this lawsuit on behalf of herself and all others similarly situated. Plaintiff Reichert received a notice, dated March 26, 2021, that her PII and PHI had been compromised by a cyberattack and confirmed that data involved in the cyberattack contained patient data, stolen from Apple Valley Clinic because its IT service provider, Netgain Technology, LLC experienced the Data Breach.

12. Defendant Netgain Technology, LLC is a United States cloud-based IT services provider based in St. Cloud, Minnesota and incorporated in Delaware.

FACTUAL BACKGROUND

13. Netgain was founded in 2000 under the premise "that there had to be a better way to implement, manage and support IT."[2] As a provider of new and innovative IT services and solutions, Netgain claims to have revolutionized the industry for support and help desk experiences for organizations across various industries. By 2004, only a few years after its inception, Netgain found its niche in specialized healthcare service and support. As a provider of cybersecurity solutions, among other IT services, Netgain has both the duty and

[2] https://netgaincloud.com/about-us/history/ (last accessed May 26, 2021).

the expertise to safeguard the data of the organizations receiving its services. Plaintiff and Class members had a reasonable expectation that Netgain would safely and securely store their PII and especially their PHI from digital theft and misuse.

14. As detailed more fully below, Netgain failed store the PII and PHI safely and securely entrusted to it and failed to prevent it from being compromised during the Data Breach.

A. The Data Breach

15. Netgain claims to be the industry standard for secure and scalable IT as a Service for accounting and healthcare businesses.[3] As such, Netgain is well aware the accounting and healthcare industries process the most valuable data for cybercriminals.

16. In fact, Netgain touts its data security measures are like "Housing user data within the granite confines of a former Federal Building" which "ensures a level of structural stability that our clients trust."[4] Yet, while its customers reasonably believed their data was safe within Netgain's confines, between September 2020 and November 2020 Netgain allowed cyber criminals to infiltrate Netgain's security walls.

17. In late September through December 2020, Netgain was subjected to a ransomware attack that targeted Netgain's domain controllers, which manage networks of thousands of servers. Included in the ransomware attack was the PII and PHI provided to Netgain by certain of its clients. Shortly thereafter, Netgain began emailing its clients that it

[3] https://netgaincloud.com/about-us/ (last accessed May 26, 2021).
[4] *Id.*

was going to shut down data centers in an effort to isolate the ransomware and rebuild the affected systems.

18. In December 2020, Netgain began notifying its clients their information may have been compromised in the ransomware attack.

19. For example, in March 2021, Apple Valley Clinic notified nearly 158,000 patients that on "December 2, 2020, we were notified by Netgain that its systems had been compromised by a cyberattack." It was only on "January 29, 2021 after the Netgain systems were restored" that Netgain sent a "confirmation that the data involved in the cyberattack contained patient data."[5]

20. Additional notifications went out, in a Notification Letter to other Netgain clients such as Woodcreek Provider Services, LLC. Netgain reported "a security incident that involved unauthorized access to portions of the Netgain environment which Netgain had discovered in late November 2020 but may have occurred as early as September 2020." The cyber criminals launched a ransomware attack, encrypting a portion of Netgain's internal systems and a subset of the PII and PHI of Netgain's clients. In response, Netgain reported it took measures to contain the threat, including disabling external and internal network pathways and taking client services offline.[6]

[5] https://www.applevalleymedicalcenter.com/contents/press-release (last accessed May 26, 2021).
[6] https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/Supporting_Law_Enforcement/WoodcreekProviderServicesLLC.2021-02-17.pdf (last accessed May 26, 2021).

21. Various notices have indicated the stolen PII and PHI included full names, dates of birth, bank account and routing numbers, Social Security numbers, driver's license numbers, medical records, health insurance policy numbers, and employee health information. Plaintiff Reichert's notice indicated the data involved in the "cyberattack on Netgain's system included the following types of personal information: names, dates of birth, social security numbers, bank account and routing numbers, patient billing information and medical information, such as medical symptoms and diagnoses."

22. Although Plaintiff's notice apprised her that the breach was known at least by December 2, 2020, she was not sent notice of it until March 26, 2021. Plaintiff was not able to take action to secure her PII/PHI and mitigate any associated risks or harm until over four months after the breach occurred.

1. Data Breaches Lead to Identity Theft and Cognizable Injuries.

23. The personal, health, and financial information of consumers, such as Plaintiff's and Class members', is valuable and easily commoditized.

24. The ramifications of Defendant's failure to keep Plaintiff's and Class members' PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

25. According to industry experts, one out of four data breach notification recipients become a victim of identity fraud.

26. Stolen PII/PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

27. Once PII and PHI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends, and colleagues of the original victim.

28. Indeed, Defendant has specifically recognized "The Real Cost of Data Breach for Financial Services" in a recent March 3, 2020 Netgain Blog post by Kris Tufto. Recognizing that aside from healthcare data, financial services data "proves to be some of the most valuable data."[7] Netgain recognized that hacking and malware "remain the primary cause of data breaches" which continue to grow and that the average cost for an organization is approximately $8.18 million in direct and indirect costs.[8] Failure to heed to its own data security warnings, Defendant has failed to adequately secure its own clients' data, including Plaintiff's and Class members' PII and PHI.

29. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

---

[7] https://netgaincloud.com/blog/how-costly-is-a-data-breach/ (last accessed May 26, 2021)
[8] *Id.*

30. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and Class members that their PII and PHI had been stolen.

31. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

32. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII and PHI to others who do the same.

33. Moreover, in light of the current COVID-19 pandemic, Plaintiff's sensitive information could be used to fraudulently obtain any emergency stimulus or relief payments or any additional forms monetary compensation, unemployment and/or enhanced unemployment benefits.

34. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

35. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII and PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future

inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

36. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII and PHI. To protect themselves, Plaintiff and Class members (and the business entities whose information was breached) will need to be remain vigilant against unauthorized data use for years or even decades to come.

37. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In a recent FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point: Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.

38. Recognizing the high value consumers place on their PII and PHI, many companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share and who ultimately receives the information. And, by making the transaction transparent, consumers—not criminals—will be compensated.[9]

39. Consumers place a high value on their PII and a greater value on their PHI, in addition to the privacy of same. Research shows how much consumers value their data privacy, and the amount is considerable.

[9] *See* Steve Lohr, *You Want My Personal Data? Reward Me for It*, N. Y. Times, July 18, 2010, *available at* http://www.nytimes.com/2010/07/18/business/18unboxed.html (last accessed May 26, 2021).

40. By virtue of the Data Breach here and unauthorized release and disclosure of the PII and PHI of Plaintiff and the Class, Defendant has deprived Plaintiff and the Class of the substantial value of their PII and PHI, to which they are entitled. As previously alleged, Defendant failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

41. As a cybersecurity expert, Defendant is aware of the potential harm caused by this data theft, and even offers cyber security best practices tips.[10] In fact, in a March 24, 2021 blog entitled "What we learned as a ransomware victim – so you don't become one," Netgain's Vice President of Client Operations, Patrick Williamson admits Netgain identified "additional opportunities to strengthen our security posture in a continuous journey with an ongoing commitment to ensure this remains top-of- mind."[11] Netgain, as a company profiting from its cybersecurity expertise and services, understands better than most how important data security is and the ongoing nature of maintaining the latest technology and protocols for cyber security.

42. According to the Federal Trade Commission ("FTC"), unauthorized PII and PHI disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[12]

---

[10] *See* Kris Tufto, How Costly is a Data Breach, *available at* https://netgaincloud.com/blog/how-costly-is-a-data-breach/ (last accessed May 26, 2021).
[11] *See* What we learned as a ransomware victim – so you don't become one, *available at* https://netgaincloud.com/blog/what-we-learned-as-a-ransomware- victim-so-you-dont-become-one/ (last accessed May 26, 2021).
[12] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last accessed May 26, 2021).

43. Identity theft associated with data breaches is particularly pernicious because the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

44. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

45. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

46. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiff's and other Class members' PII and PHI, Plaintiff and the other Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, inter alia, (i) the untimely and inadequate notification of the Data Breach, (ii) the resulting immediate increased risk of future ascertainable losses, economic damages and other actual injury and harm, (iii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; and (iv) out-of-pocket expenses for securing identity theft protection and other similar necessary services.

47. Plaintiff Reichert received treatment at an Allina Health Clinic, the Apple Valley Clinic, which used Defendant as a third-party hosting provider.

48. According to the Notice, Plaintiff's PHI, stored on Defendant's system was determined to be impacted.

CLASS DEFINITION AND ALLEGATIONS

49. Plaintiff bring this class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of a nationwide class:

> All persons residing in the United States who had their PII and/or PHI hosted by Netgain compromised as a result of the Data Breach.

Excluded from the Class is: (i) Defendant and its officers, directors, affiliates, parents, and subsidiaries; (ii) the Judge presiding over this action; and (iii) any other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Breaches.

50. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

51. The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes hundreds of thousands of Defendant's customers who have been damaged by Defendant's conduct as alleged herein. The precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records.

52. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

a. whether Defendant engaged in the wrongful conduct alleged herein;

b. whether the alleged conduct constitutes violations of the laws asserted;

c. whether Defendant owed Plaintiff and the other Class members a duty to adequately protect their PII and PHI;

d. whether Defendant breached its duty to protect the personal and financial data of Plaintiff and the other Class members;

e. whether Defendant knew or should have known about the inadequacies of their data protection, storage, and security;

f. whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and the other Class members' PI and /PHI from unauthorized theft, release, or disclosure;

g. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendant's offices;

h. whether Defendant had the proper computer systems to safeguard and protect Plaintiff's and the other Class members' PII and PHI from unauthorized theft, release or disclosure;

i. whether Defendant breached its promise to keep Plaintiff's and the Class members' PII and PHI safe and to follow federal data security protocols;

j. whether Defendant's conduct was the proximate cause of Plaintiff's and the

other Class members' injuries;

k. whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

l. whether Plaintiff and the other Class members suffered ascertainable and cognizable injuries as a result of Defendant's conduct;

m. whether Plaintiff and the other Class members are entitled to recover actual damages and/or statutory damages; and

n. whether Plaintiff and the other Class members are entitled to other appropriate remedies, including injunctive relief.

53. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiff on behalf of herself and the other Class members. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

54. Plaintiff's claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class members in a similar manner.

55. Plaintiff will fairly and adequately protect the interests of the members of the Class, have retained counsel experienced in complex consumer class action litigation, and intend to prosecute this action vigorously. Plaintiff has no adverse or antagonistic interests to those of the Class.

56. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

57. Plaintiff restates and realleges all proceeding factual allegations above and hereafter as if fully set forth herein.

58. Upon gaining access to the PII and PHI of Plaintiff and members of the Class, Defendant owed to Plaintiff and the Class a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties. Pursuant to this duty, Defendant was required to design, maintain, and test their security systems to ensure that these systems were reasonably secure and capable of protecting the PI and /PHI of Plaintiff and the Class. Defendant further owed to Plaintiff and the Class a duty to implement systems and procedures that would detect a

breach of their security systems in a timely manner and to timely act upon security alerts from such systems.

59. Defendant owed this duty to Plaintiff and the other Class members because Plaintiff and the other Class members compose a well-defined, foreseeable, and probable class of individuals whom Defendant should have been aware could be injured by Defendant's inadequate security protocols. Defendant actively solicited clients who entrusted Defendant with Plaintiff's and the other Class members' PII and PHI when obtaining and using IT services and products. To facilitate these services, Defendant used, handled, gathered, and stored the PII and PHI of Plaintiff and the other Class members. Attendant to Defendant's solicitation, use and storage, Defendant knew of its inadequate and unreasonable security practices with regard to their computer/server systems and also knew that hackers and thieves routinely attempt to access, steal and misuse the PII and PHI that Defendant actively solicited from clients who entrusted Defendant with Plaintiff and the other Class members data. As such, Defendant knew a breach of its systems would cause damage to its clients and Plaintiff and the other Class members. Thus, Defendant had a duty to act reasonably in protecting the PII and PHI of its clients.

60. Defendant also owed a duty to timely and accurately disclose to its clients and Plaintiff and the other Class members, the scope, nature, and occurrence of the Data Breach. This disclosure is necessary so Plaintiff and the other Class members can take appropriate measures to avoid unauthorized use of their PII and PHI, accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial institutions about compromise or possible

compromise, obtain credit monitoring services, and/or take other steps in an effort to mitigate the harm caused by the Data Breach and Defendant's unreasonable misconduct.

61. Defendant breached its duty to Plaintiff and the other Class members by failing to implement and maintain security controls that were capable of adequately protecting the PII/PHI of Plaintiff and the other Class members.

62. Defendant also breached its duty to timely and accurately disclose to the clients, Plaintiff and the other Class members, that their PII and PHI had been or was reasonably believed to have been improperly accessed or stolen.

63. Defendant's negligence in failing to exercise reasonable care in protecting the PII and PHI of Plaintiff and the other Class members is further evinced by Defendant's failure to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when the Data Breach was disclosed.

64. The injuries to Plaintiff and the other Class members were reasonably foreseeable to Defendant because laws and statutes, and industry standards require Defendant to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiff's and the other Class members' PII and PHI.

65. The injuries to Plaintiff and the other Class members also were reasonably foreseeable because Defendant knew or should have known that systems used for safeguarding PII and PHI were inadequately secured and exposed consumer PII and PHI to being breached, accessed, and stolen by hackers and unauthorized third parties. As such,

Defendant's own misconduct created a foreseeable risk of harm to Plaintiff and the other Class members.

66. Defendant's failure to take reasonable steps to protect the PII and PHI of Plaintiff and the other members of the Class was a proximate cause of their injuries because it directly allowed thieves easy access to Plaintiff's and the other Class members' PII and PHI. This ease of access allowed thieves to steal PII and PHI of Plaintiff and the other Class members, which could lead to dissemination in black markets through the "dark web."

67. As a direct proximate result of Defendant's conduct, Plaintiff and the other Class members have suffered theft of their PII and PHI. Defendant allowed thieves access to Class members' PII and PHI, thereby decreasing the security of Class members' financial and health accounts, making Class members' identities less secure and reliable, and subjecting Class members to the imminent threat of identity theft. Not only will Plaintiff and the other members of the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

68. Defendant's conduct warrants moral blame because Defendant actively solicited its services to its clients, wherein it used, handled and stored the PII and PHI of Plaintiff and the other Class members without disclosing that its security was inadequate and unable to protect the PII and PHI of Plaintiff and the other Class members. Holding Defendant accountable for its negligence will further the policies embodied in such law by incentivizing larger IT service providers to properly secure sensitive consumer information and protect the consumers who rely on these companies every day.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Nationwide Class)

69. Plaintiff restates and realleges all proceeding factual allegations above and hereafter as if fully set forth herein.

70. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Netgain for failing to use reasonable measures to protect PII/PHI. Various FTC publications and orders also form the basis of Netgain's duty.

71. Netgain violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with the industry standards. Netgain's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtained and stored and the foreseeable consequences of a data breach.

72. Netgain's violation of Section 5 of the FTC Act constitutes negligence *per se*.

73. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

74. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

75. As a direct and proximate result of Netgain's negligence, Plaintiff and Class members have been injured as described herein and throughout this Complaint, and are

entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Nationwide Class)

76. Plaintiff restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

77. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

78. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class members' PII and PHI, including whether Netgain is currently maintaining data security measures adequate to protect Plaintiff's and Class members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Netgain's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her PII and PHI and remains at imminent risk that further compromises of her PII and PHI will occur in the future.

79. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Netgain owes a legal duty to secure consumers' PII and PHI and to timely notify consumers of a data breach under the common law, and Section 5 of the FTC Act; and

b. Netgain continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII and PHI.

80. This Court also should issue corresponding prospective injunctive relief requiring Netgain to employ adequate security protocols consistent with law and industry standards to protect consumers' PII and PHI.

81. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Netgain. The risk of another such breach is real, immediate, and substantial. If another breach at Netgain occurs, Plaintiff and Class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

82. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Netgain if an injunction is issued. Plaintiff and Class members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Netgain of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Netgain has a pre-existing legal obligation to employ such measures.

83. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at

Netgain, thus eliminating the additional injuries that would result to Plaintiff and consumers whose PII/PHI would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying the Class as requested in this Complaint;

b. Appointing Plaintiff as Class Representative and undersigned counsel as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged in this Complaint;

d. Enjoining Defendant's conduct and requiring Defendant to implement proper data security practices, specifically:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

   iii. requiring Defendant to delete, destroy, and purge the PII and PHI of Plaintiff and the Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class members;

   iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal

identifying information of Plaintiff's and the Class members' PII/PHI;

v. prohibiting Defendant from maintaining Plaintiff's and the Class members' PII and PHI on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems;

vii. on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII and PHI, as well as protecting the PII/PHI of Plaintiff and the Class members;

xiii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach

when it occurs and what to do in response to a breach;

xiv. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting PII and PHI;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

xviii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xix. requiring Defendant to design, maintain, and test its computer systems to ensure that PII/PHI in its possession is adequately secured and protected;

xx. requiring Defendant to disclose any future data breaches in a timely and accurate manner;

xxi. requiring Defendant to implement multi-factor authentication requirements;

xxii. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxiii. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class members.

e. Awarding Plaintiff and Class members damages;

f. Awarding Plaintiff and Class members pre-judgment and post- judgment interest on all amounts awarded;

g. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

Plaintiff Susan Reichert, on behalf of herself individually and the putative Class, demands a trial by jury on all issues so triable.

Respectfully submitted,

CHESTNUT CAMBRONNE PA

Dated: May 28, 2021

By: *s/ Bryan L. Bleichner*

Bryan L. Bleichner (MN #0326689)
Jeffrey D. Bores (MN #227699)
Christopher P. Renz (MN #0313415)
17 Washington Ave. N., Suite 300
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
jbores@chestnutcambronne.com
crenz@chestnutcambronne.com

Nathan D. Prosser (MN #0329745)
Anne T. Regan (MN #0333852)
HELLMUTH & JOHNSON PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: 952-941-4005
Facsimile: 952-941-2337
nprosser@hjlawfirm.com
aregan@hjlawfirm.com

Terence R. Coates*
Justin C. Walker*
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
bmarkovits@msdlegal.com
tcoates@msdlegal.com

ATTORNEYS FOR PLAINTIFF

**Pro Hac Vice Forthcoming*